ISSN 1066-369X, Russian Mathematics, 2017, Vol. 61, No. 11, pp. 53–59. © Allerton Press, Inc., 2017.
Original Russian Text © F.F. Sharifullina, 2017, published in Izvestiya Vysshikh Uchebnykh Zavedenii. Matematika, 2017, No. 11, pp. 60–67.

# On Powersmooth Numbers

**F. F. Sharifullina**[1*]

[1] *Kazan Federal University*
*ul. Kremlyovskaya 18, Kazan, 420008 Russia*

Received June 27, 2016

**Abstract**—A natural number $n$ is called $y$-smooth ($y$-powersmooth, respectively) for a positive number $y$ if every prime (prime power) dividing $n$ is bounded from above by $y$. Let $\psi(x,y)$ and $\psi^*(x,y)$ denote the quantity of $y$-smooth and $y$-powersmooth integers restricted by $x$, respectively. In this paper we investigate function $\psi^*(x,y)$ in general. We derive formulas for finding exact calculation of $\psi^*(x,y)$ for large $x$ and relatively small $y$ and give theoretical estimates for this function and for a function of the greatest powersmooth integer. This results can be used in the cryptography and number theory to estimate the convergence of factorization algorithms.

**DOI:** 10.3103/S1066369X1711007X

Keywords: *smooth integers, powersmooth integers, factorization, estimates for cryptographic algorithms, Lenstra's elliptic curve factorization method, Pollard's $(p-1)$-factorization algorithm, RSA.*

## INTRODUCTION

Let $y$ be a positive number. A positive integer $n$ is called *$y$-smooth* if any prime divisor $p$ of $n$ satisfies the inequality $p \le y$. A natural number $n$ is called *$y$-powersmooth*, if any divisor $p^k$ of $n$ for a prime $p$ satisfies $p^k \le y$.

Every $y$-powersmooth number is $y$-smooth. The converse is not true and there exist $y$-smooth numbers which are not $y$-powersmooth. For example, 48 is 10-smooth, but not 10-powersmooth. Powersmooth number means $y$-powersmooth unless otherwise specified.

We denote by $\psi(x,y)$ the number of $y$-smooth integers less than or equal to $x$, and by $\psi^*(x,y)$ the number of $y$-powersmooth integers less than or equal to $x$. This implies $\psi^*(x,y) \le \psi(x,y)$ for all $x$ and $y$.

The function $\psi^*(x,y)$ plays an essential role in choosing parameters of Lenstra's elliptic curve factorization method. For the convergence of the Lenstra method is suffices that the the number of points on the elliptic curve chosen be $y$-powersmooth number, where $y$ is a factor of the number factorizing [1].

We note that the exact calculation of both functions $\psi(x,y)$ and $\psi^*(x,y)$ is a hard computational problem, so in practice these functions are calculated by approximate algorithms. At the present time there are known many algorithms that allow to approximate function $\psi(x,y)$ [2]. This does not hold for $\psi^*(x,y)$ and often its use in applications is replaced by $\psi(x,y)$ [3]. For example, in [4] (P. 338) the convergence of the Lenstra factorization algorithm is performed by $\psi(x,y)$ instead of $\psi^*(x,y)$.

Meanwhile, functions $\psi^*(x,y)$ and $\psi(x,y)$ have different behavior. In the graph below we draw curves for $\psi(x,y)$ (top line) and $\psi^*(x,y)$ at $y=6$ and $x=6^k$, $k=1,2,3,4$ (Figure):

One can see that function $\psi(x,y)$ is growing more rapidly, whereas the function $\psi^*(x,y)$ becomes constant starting with certain $x$. This is a consequence of the fact that at a fixed $y$ the number of of all $y$-smooth numbers is infinite, while the number of $y$-powersmooth numbers is finite and therefore there is a greatest $y$-powersmooth number.

* E-mail: farida.f.sharifullina@mail.ru.